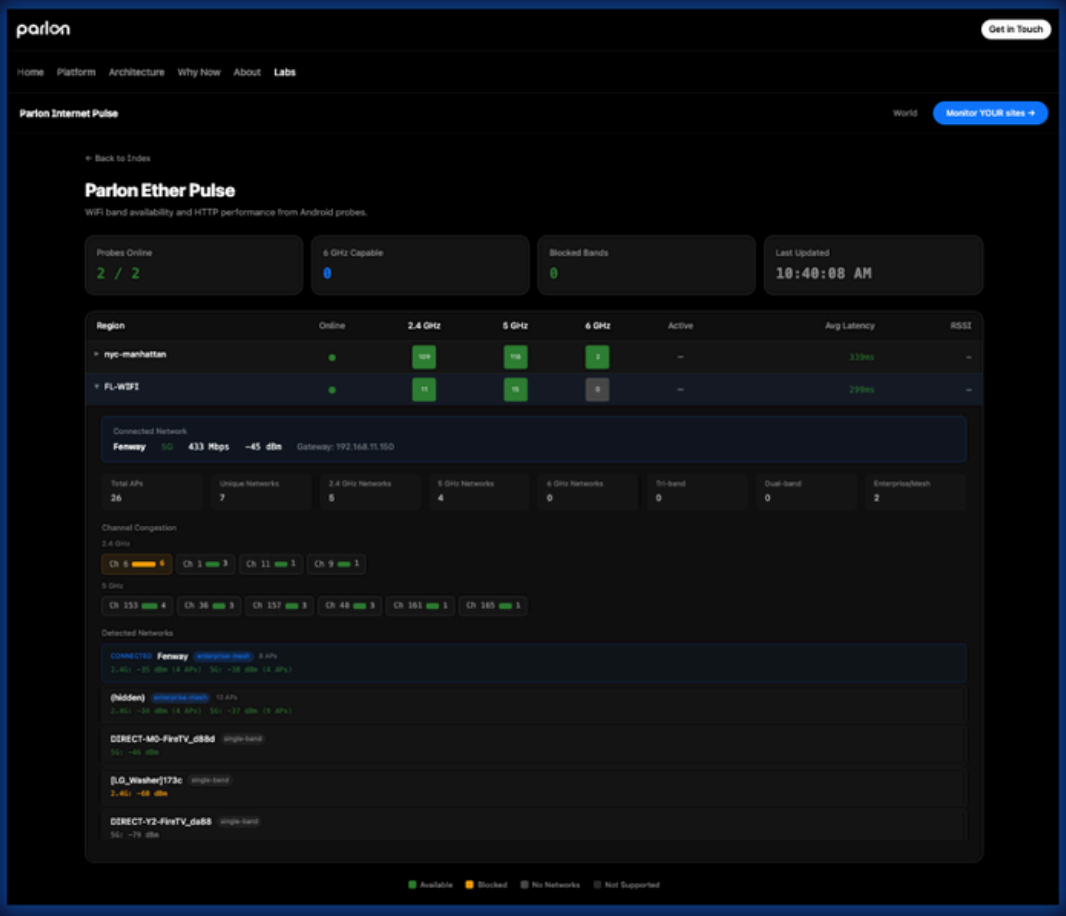
parlon

Android as a Probe

Zero-hardware monitoring infrastructure

Turn any Android phone into a distributed WiFi scanner and HTTP performance probe — no root, no MDM, no custom hardware



parlon.io

Why Android phones are the ideal probe hardware

Traditional monitoring probes require purpose-built hardware, custom firmware, or expensive appliances.Android phones are production-grade sensor platforms that already exist in every drawer, closet, and IT surplus bin.

$0	3	5 min	0
Hardware Cost (use existing)	WiFi Bands (2.4/5/6 GHz)		Root / MDM Required

Built-in Capabilities

- **Tri-band WiFi radios.** Scan 2.4 GHz, 5 GHz, and 6 GHz (WiFi 6E). Detect every nearby network with SSID, BSSID, frequency, channel, signal strength.
- **Full HTTP stack.** Real HTTP HEAD/GET requests through the complete network stack. Measures what users actually experience.
- **Cellular fallback**. If WiFi goes down, the phone reports over cellular. The probe doesn't go dark when the monitored network fails.
- **Battery + USB power.** Survives power blips on internal battery. Runs indefinitely plugged in. No UPS needed.

vs. Dedicated Hardware Probes

vs. Raspberry Pi / Custom IoT
Requires WiFi dongle, SD card, SSH, OS updates. Phones have better radios, better power management, and a touch UI for config.

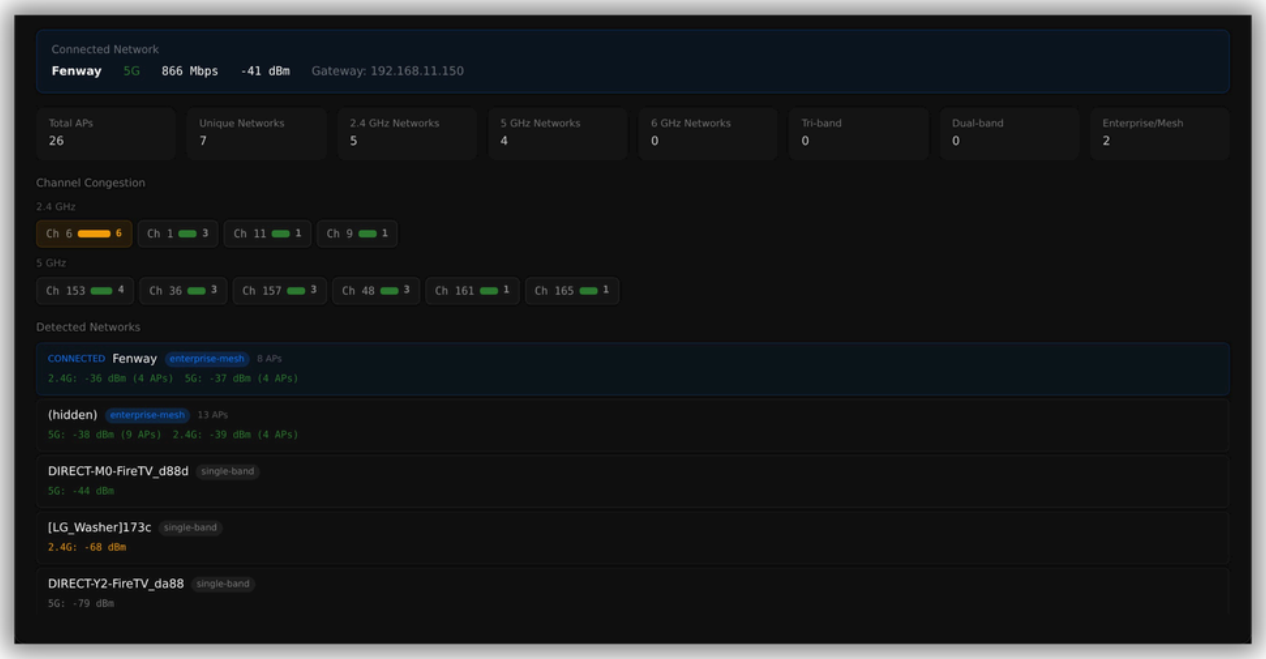
vs. Enterprise Sensors (Ekahau, Cisco DNA)
$1,500-$5,000 per unit plus licensing. Android: install APK on $100 phone. Same capability, 10-50x cheaper.

vs. Network TAPs / Appliances
Require rack space, network access, expertise. Phone sits on a shelf. No infrastructure changes.

The economics: Refurbished Android phone: $50-100. Enterprise WiFi sensor: $1,500-5,000. Both scan WiFi bands and run HTTP checks. The phone also has a screen, battery, and cellular fallback.

How the Android probe works

The Parlon Ether Pulse APK transforms any Android 10+ phone into a fully autonomous monitoring agent.



Real data from an Android probe: connected network, area intelligence, channel congestion, and detected networks

Every 5 minutes, the probe:

#	Action	Data Collected	Technical Detail
1	WiFi Scan	All nearby networks: SSID, BSSID, frequency, channel, RSSI	WifiManager.scanResults API. Within Android's 4-scan-per-2-min limit.
2	Connection Telemetry	Connected SSID, band, link speed, RSSI, gateway IP	WifiInfo + DhcpInfo APIs. No root required.
3	HTTP Probes	Response time to 10 major sites	HTTP HEAD, 10-second timeout. Real application-layer latency.
4	Band Cycling	Per-band latency: 2.4/5/6 GHz	WifiNetworkSuggestion API. Waits up to 15s for band association.
5	POST to API	Single JSON payload	HTTPS POST to /wifi/api/ingest. Authenticated with probe secret.

Three-layer resilience architecture

Android aggressively kills background processes. The probe uses three independent mechanisms for continuous operation:

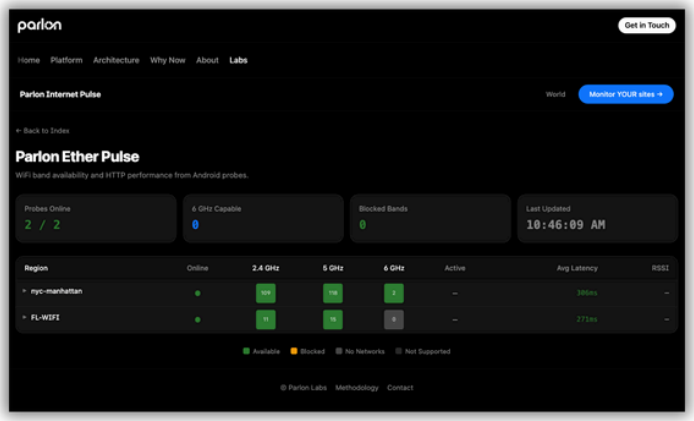
Layer 1: Foreground Service + WakeLock
Visible foreground service with persistent notification. PARTIAL_WAKE_LOCK prevents CPU sleep during Doze. START_STICKY for auto-restart.

Layer 2: BootReceiver
Listens for BOOT_COMPLETED. After any reboot, the probe service automatically restarts without user intervention.

Layer 3: Work Manager Fallback
Periodic task every 15 min. If aggressive OEM battery managers (Xiaomi, Huawei, Samsung) kill the service, WorkManager detects and restarts it.

What Android probes power today

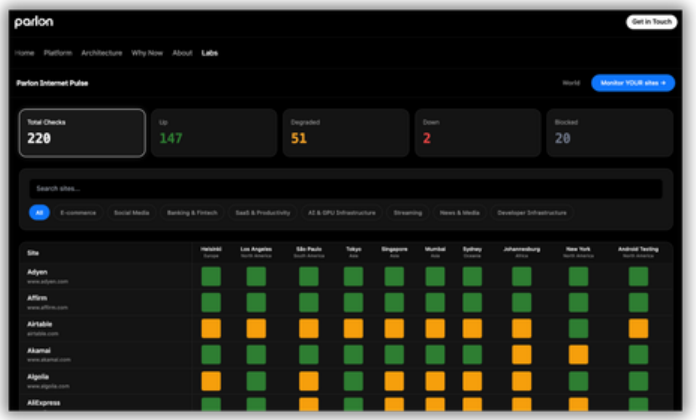
Ether Pulse: WiFi Intelligence



Ether Pulse dashboard powered by Android probe data

- **Band availability monitoring.** Real-time 2.4/5/6 GHz status at each location.
- **Network intelligence.** Classify all nearby networks by type and capability.
- **Channel congestion.** Which channels are overcrowded vs. clear.
- **HTTP latency from WiFi.** Real client-side performance measurement.

Cross-correlation with PIP



PIP: when latency spikes, was it WiFi or upstream?

- **Root cause isolation.** PIP shows upstream. Ether Pulse shows WiFi. Together: full path.
- **Full-path visibility.** VPS probes (clean network) + WiFi probes (real environment).
- **Same dashboard.** One interface for internet health + WiFi health.
- **Android Testing column.** Compare real-device WiFi performance vs. datacenter.

Real-world use cases

Android probes solve monitoring problems that traditionally required expensive hardware, truck rolls, or simply went unmonitored.

Hospital Floor WiFi for Medical Devices

HEALTHCARE IT

"Vitals monitors keep dropping off WiFi on the 3rd floor ICU. We can't have gaps in patient telemetry."

Deploy phones	Monitor 2.4 GHz	Find interference	Relocate AP channel	Verify stability
1 per ICU wing, USB-powered	Where medical IoT lives	Ch 1: 12 networks competing	Move to clear Ch 11	Continuous 24/7 monitoring

Result: Zero dropped connections in 30 days. Continuous proof that medical-grade WiFi SLA is met.

Remote Worker VPN Troubleshooting

ENTERPRISE IT / HELP DESK

"VPN is slow" is our #1 help desk ticket. We can't see the employee's home WiFi environment."

Ship phone to employee	Scan home WiFi	HTTP latency data	Root cause: WiFi	Recommend fix
Pre-configured, self-install	8 neighbor networks on same channel	WiFi: 400ms vs. direct: 50ms	Not VPN, not ISP	Switch to 5 GHz band

Result: Resolved 60% of "VPN is slow" tickets without escalation. Data proves WiFi is the bottleneck.

Co-Working Space WiFi as a Service

FACILITY OPERATIONS

"We charge premium rates. WiFi quality is a key differentiator. But we have zero visibility into what members experience."

Deploy per floor	Measure client-side	Dashboard for ops	Proactive fixes	Marketing proof
Phones at hot desks	Real latency, not AP stats	Per-floor WiFi quality score	Before member complaints	"99.8% WiFi uptime"

Result: WiFi quality becomes a measurable, marketable differentiator. Retention improves with proactive issue resolution.

MSP Multi-Client Remote Monitoring

MANAGED SERVICE PROVIDER

"We manage networks for 40 clients. Every WiFi complaint means a truck roll. We need remote visibility."

1 phone per client	Fleet dashboard	Alert on anomalies	Triage remotely	Fix without driving
Ship, self-install, done	All 40 clients at a glance	Client #12: latency spike	Channel congestion, not AP failure	Remote channel change

Result: 70% reduction in WiFi-related truck rolls. Monthly health reports from real data, not guesswork.

Smart Building IoT Connectivity Assurance

BUILDING AUTOMATION

"Our building has 200 WiFi sensors for HVAC, lighting, and access control. Some go offline randomly."

Probes per zone	Track 2.4 GHz	Correlate dropoffs	Identify pattern	Schedule quiet channel
Match IoT sensor locations	Where IoT devices connect	With congestion spikes	Lunch hour = max inter ference	Reserve band for IoT

Result: IoT reliability went from 94% to 99.7%. Identified time-of-day interference pattern invisible to the controller.

Deploy anywhere in 5 minutes

1. **Get a Phone**
   Any Android 10+. Refurb Pixel: ~$80
2. **Install APK**
   Download from API, grant permissions
3. **Configure**
   Region, API URL, secret
4. **Plug In & Go**
   Data flows within 5 minutes

Deployment scenarios

Scenario	Placement	What You Learn	Scale
Office floors	1 phone per floor, USB	Per-floor WiFi quality and channel congestion	5-20 phones
Retail locations	Behind counter	Guest WiFi from customer perspective	1 per store
MDU / Property	Common areas	Managed WiFi SLA compliance	1-3 per building
Remote offices	Near workspace	Remote worker WiFi environment	1 per worker
ISP premises	Near router	WiFi vs. uplink diagnosis	Ship to customer

Technical requirements

- **Android 10+** (API 29) for modern scan and suggestion APIs.
- **Location permission** (required by Android for WiFi scanning). Location data not transmitted.
- **WiFi connection** to monitored network. Cellular for fallback.
- **USB power** recommended for continuous operation.
- **No root, no MDM.** Standard APK install.
- **~15 MB APK.** No local data retention — streamed to API.

Bottom line: Every organization has old Android phones. Every location has a power outlet. That's all you need for continuous WiFi monitoring — from every site, every floor, every 5 minutes.